# Two Concepts of Group Privacy

Loi, Michele ; Christen, Markus

Abstract: Luciano Floridi was not the first to discuss the idea of group privacy, but he was perhaps the first to discuss it in relation to the insights derived from big data analytics. He has argued that it is important to investigate the possibility that groups have rights to privacy that are not reducible to the privacy of individuals forming such groups. In this paper, we introduce a distinction between two concepts of group privacy. The first, the "what happens in Vegas stays in Vegas" privacy (in the following: WHVSV privacy), deals with confidential information shared with the member of a group and inaccessible to (all or a specific group of) outsiders. The second, to which we shall refer as inferential privacy, deals with the inferences that can be made about a group of people defined by a feature, or combination thereof, shared by all individuals in the group. We show why we unreservedly agree with Floridi that groups can have a form of privacy that amounts to more than the mere fact of being sets of individuals each of whom has individual privacy; moreover, like Floridi, we find it plausible that at least some groups (those satisfying our definition of type-a groups) may have a right to a species of group privacy (that is, WHVSV privacy) as groups (and not just as individuals who belong to those groups). However, by turning our attention to the context of big data analytics, we show that the relevant, new notion of group privacy is one of inferential privacy. We argue that an absolute right (either of individuals or groups) to inferential privacy is implausible. We also show that many groups generated algorithmically (those satisfying our definition of type-b groups) cannot be right holders as groups (unless they become type-a groups).

DOI: https://doi.org/10.1007/s13347-019-00351-0



Originally published at:
Loi, Michele; Christen, Markus (2020). Two Concepts of Group Privacy. Philosophy Technology, 33(2):207-224.
DOI: https://doi.org/10.1007/s13347-019-00351-0

Philosophy & Technology
https://doi.org/10.1007/s13347-019-00351-0

RESEARCH ARTICLE

# Two Concepts of Group Privacy

Michele Loi[1] · Markus Christen[2]

Received: 28 September 2018 / Accepted: 2 May 2019/Published online: 29 May 2019


## Abstract

Luciano Floridi was not the first to discuss the idea of group privacy, but he was perhaps the first to discuss it in relation to the insights derived from big data analytics. He has argued that it is important to investigate the possibility that groups have rights to privacy that are not reducible to the privacy of individuals forming such groups. In this paper, we introduce a distinction between two concepts of group privacy. The first, the "what happens in Vegas stays in Vegas" privacy (in the following: WHVSV privacy), deals with confidential information shared with the member of a group and inaccessible to (all or a specific group of) outsiders. The second, to which we shall refer as inferential privacy, deals with the inferences that can be made about a group of people defined by a feature, or combination thereof, shared by all individuals in the group. We show why we unreservedly agree with Floridi that groups can have a form of privacy that amounts to more than the mere fact of being sets of individuals each of whom has individual privacy; moreover, like Floridi, we find it plausible that at least some groups (those satisfying our definition of type-a groups) may have a right to a species of group privacy (that is, WHVSV privacy) as groups (and not just as individuals who belong to those groups). However, by turning our attention to the context of big data analytics, we show that the relevant, new notion of group privacy is one of inferential privacy. We argue that an absolute right (either of individuals or groups) to inferential privacy is implausible. We also show that many groups generated algorithmically (those satisfying our definition of type-b groups) cannot be right holders as groups (unless they become type-a groups).

**Keywords** Luciano Floridi · Group privacy · Privacy · Big data · Data analytics · AI · Inferential privacy

✉ Michele Loi
Michele.loi@uzh.ch

Markus Christen
christen@ethik.uzh.ch

[1] Institute of Biomedical Ethics and the History of Medicine, University of Zurich, Zurich, Switzerland

[2] Digital Society Initiative, University of Zurich, Zurich, Switzerland

## 1 Introduction

Luciano Floridi was not the first to discuss the idea of group privacy, but he was perhaps the first to discuss it in relation to the insights derived from big data analytics (Floridi 2014, 2016). He has argued that it is important to investigate the possibility that groups have rights to privacy that are not reducible to the privacy of individuals forming such groups.[1] He has significantly contributed to advancing the view that the protection of the privacy of a group should also be a goal of privacy regulation, in response to advances in big data technology. He has objected to the "individualism" of most data protection regulations, for example, the EU General Data Protection Regulation. This is centered on identifiable individuals,[2] where individuals are defined as "natural persons" (Com (2012) 10 final 2012/0010, cited in Floridi 2016). There are risks for privacy, Floridi claims, resulting from the assumption that if the privacy of individuals is taken care of, the privacy of groups will take care of itself. This warrants the philosophical exploration of theories of group privacy, which conceptualize group privacy as the privacy of a group which is not achieved, automatically, by protecting the individual privacy of all members of a group. Since Floridi does not say clearly what defines a group (as opposed to a mere set of items), by group, we mean both:

- Groups consisting of natural persons with an interaction history and/or collective goals in the sense of displaying some meaningful form of agency, as a group, e.g., through intentional coordination, or at least awareness of themselves as a group, with which they identify. (Type-a groups.)
- Groups consisting of natural persons with one or more features in common, who do not have the property in (a) setting aside the trivial case of shared goals, which are pursued without a common plan, or for the common good; e.g., smokers share the goal to smoke. (Type-b groups.)

In this paper, we introduce a distinction between two concepts of group privacy. The first, the "what happens in Vegas stays in Vegas" privacy (in the following: WHVSV privacy), deals with confidential information shared with the member of a group and inaccessible to (all or a specific group of) outsiders. The second, to which we shall refer as inferential privacy, deals with the inferences that can be made about a group of people defined by a feature, shared by all individuals in the group (e.g., being a smoker).

Floridi (who does not distinguish the two kinds of groups above) argues that groups should have rights to group privacy, in a strong sense. Group privacy in a strong sense is to be distinguished from group privacy in a derivative sense, which refers to a property of a group formed by individuals each of which has individual privacy. In this paper, we partially agree and partially disagree with Floridi. Section 2 articulates the scope of our agreement with Floridi. We show that the concept of WHVSV privacy constitutes a form of group privacy in the relevant strong sense. Thus, we unreservedly

[1] In our contribution, the notion of a "group" refers to set of persons, not to groups (or sets) of any entity. We are not discussing ontological questions, e.g., whether "natural groups" exist.

[2] "Whereas the principles of protection must apply to any information concerning an identified or identifiable person" (Directive 95/46/Ec, cited in Floridi 2016).

agree with Floridi that groups can have a form of privacy that amounts to more than the mere fact of being sets of individuals each of whom has individual privacy; moreover, like Floridi, we find it plausible that at least some groups (that is, type-a groups) have a right to a species of group privacy (that is, WHVSV privacy) qua groups (and not just qua individuals who belong to those groups).

We then (Section 3) turn to inferential privacy. By turning our attention to the context of big data analytics, we analyze the possibility that the privacy of an individual is infringed through inferences made by virtue of data about other individuals who share one or more features with the first. Since all individuals that happen to share the same feature, or set of features, are exposed to similar risk deriving from the same inference being made about them, this appears to support a group right to protect the privacy of that group. We also show that typically, in the big data contexts, these groups are type-b groups.

In Section 4, we briefly consider the moral right to inferential privacy and deny the possibility of an absolute right to it, while allowing the possibility of a limited right. In Section 5, we argue that this is not a group right in the strong sense, but only—at most—a right of the individuals who happen to belong to the group.

It is important to clarify the relation between the distinction between a-groups and b-groups and our distinction between two concepts of group privacy. The two distinctions do not overlap (see Table 1, below). Our claim is not that b-groups cannot have group rights, because they are b-groups. Our claim is narrower: in the case of a b-group, it is not plausible to consider inferential privacy as the object of a group right. We remain agnostic on whether a-groups have group rights to inferential privacy and we do not examine the claim (which we have not found in the literature) that b-groups should have group rights to WHSVS privacy.

We do not claim that the two concepts of a "group" identify a sharp dichotomy. Indeed, they are more plausibly thought of as two poles in a continuum, with intermediate forms in the between. Self-awareness and organizational structure may both come in degrees. It might be difficult to define sharply how much awareness (or coordination) an a-group requires. Still, both poles play a significant heuristic function. The concepts of bald and hairy are meaningful and useful, in spite of their fuzzy nature and doubts one may have about borderline cases. Moreover, the classification of a set of individuals as an a- or b-group is not static. Consider, for example, lovers of a certain type of movies. We know that new groups of movies lovers, e.g., lovers of "African-American Crime Documentaries" or of "Scary Cult Movies from the 1980s" are identified algorithmically (Madrigal 2014). If an online platform enables some form of interaction, or elicits some form of non-trivial group self-awareness, among members of these new groups, the group may then evolve into an a-group, given our definition.

**Table 1** The two distinctions between two types of groups and two types of privacy entail four logically distinct cases. In Section 2 of this paper, we focus on (a) and in Section 3, we focus on (d). These are the focus of Floridi's article: (a) makes the idea of group privacy plausible and (d) is the alleged novelty of big data

| Types of groups/types of privacy | WHVSV privacy | Inferential privacy |
|---|---|---|
| a-groups | a | b |
| b-groups | X | d |

We do not claim that the two concepts exhaust the range of all possible distinctions between all possible concepts of privacy. They are both instances of a more general access conception of privacy, according to which privacy is a condition of restricted access to the self or information about the self.[3] We recognize that there are more expansive notions of privacy and of the right protecting it, which are particularly relevant in the sphere of online interactions. For example, the right to privacy may be considered an all-encompassing right that provides protection to almost all aspects of identity, personhood, and dignity (Hildebrandt 2013).[4] The concept of privacy as access has, however, an important history. The first definition of the right privacy, the right to be left alone (Warren and Brandeis 1890), can be considered a right to limit access to the self.

Let us briefly clarify how our contribution relates to some other in the literature. We do not adopt the conceptual framework of Alessandro Mantelero's (2016) discussion of group privacy in its entirety. Our thesis about b-groups can be reformulated, in terms of his distinction, as the claim that b-groups do not have non-aggregative collective interests in privacy, but only, at most, aggregative shared interests. However, Mantelero (2016) all concede the possibility of granting group rights to algorithmically selected groups, without further distinctions between them.[5] By contrast, we provide two arguments for denying group rights in the strong sense, when they concern the inferential privacy of b-groups.

## 2 "What Happens in Vegas Stays in Vegas" Privacy

Do groups as such have privacy, or is this only a shortcut to say that all the individuals in a group have privacy? Skepticism about the concept of group privacy is that this can only be, at most, a shortcut to say that a group is made up by entities each of which has individual privacy. This position may be motivated by a general skepticism about entities like groups and sets, of their being entities that have properties that are not the mere aggregation of those of the individuals making them up. This is not our premise. As Floridi points out, a pile of book can have the property "being too heavy to be moved by a single person" (2016, 89). Another example of a property of a set that is not a property of its members is the number of the members of the set. Floridi introduces group

[3] Following the familiar Hohfeldian decomposition into distinct incidents, rights to privacy can be decomposed into claims, liberties, immunities, and powers relative to privacy (Wenar 2011). In our view, a person's right to privacy entails, at least, (1) the claim right that other people have a duty not to access and use personal information and (2) the power right, of the person whose privacy is in question, to annul the duty corresponding to this claim right, in a way that is limited to specific persons, for specific purposes. The voluntary and informed sharing of information about the self can, simultaneously, constitute an exercise of the right to privacy, and imply a loss of privacy (the condition).

[4] This expansive conception arguably provides a better interpretation of the approach adopted by European courts. Our account is philosophical and does not aim to provide an interpretation of the law of European countries, or any other country. But the fact that we do not define privacy in terms of dignity is not incompatible with the idea that privacy, or the right to privacy (or both) are *de facto*, essential for identity, autonomy, and dignity.

[5] Pagallo grants the possibility of "a procedural right to a judicial remedy against the data controllers, processors or supervisory authorities"(2016, 163).

privacy as a property distinct from individual privacy (or the sum thereof) in the following way:

> Consider next the case in which the close friends and relatives (the group) of a deceased person decide to hold a private funeral. Attendance is by invitation only, but this is not meant to make the funeral 'exclusive'. The desired privacy may be due to a need for intimacy, for respectful quietness, to protect grieving and reflection, or perhaps because of cultural or religious customs. Whatever the reasons, in this case it seems very counterintuitive to argue that each member of the group (each close friend or relative of the deceased) has a right to a private funeral, or that the privacy demanded is just the collection of all individual privacies. It seems more reasonable to admit that we are in the presence of *a strong, social sense of group* privacy (Floridi 2016, 91 italics added).

This example is entirely plausible. Funeral participants may want to share thoughts and emotions with other participants to the funeral (so they are not private in that sense), but may also not want to exhibit to people outside that group. In fact, there are many examples of group privacy in this sense. Floridi himself mentions, as a case in point, the "defence of privacy at home – that is, within the special group represented by a family" (2016, 93). (The family is an even clearer example of a type-a group.)

We believe that the sensible concept of group privacy that applies to both the funeral and the family examples is that of WHVSV privacy, in one of its two variants, discussed below. The expression "what happens in Vegas stays in Vegas" refers to the transgressions of some tourists in Las Vegas, which they do not want their spouses, friends, and relatives at home to hear about. The idea that what happens in Vegas stays in Vegas captures the essential logical structure of this form of privacy: sharing experiences, knowledge, or emotions with insiders, creating a barrier against the gaze and judgment of outsiders.

WHVSV privacy captures the form of privacy that matters in ordinary forms of confidentiality and intimacy, which Floridi himself (2016, 96) discusses in relation to examples involving type-a groups. Consider a situation in which a group (e.g., bachelors or bachelorettes) enjoys an experience of group privacy. WHVSV is a genre with different species, two of which we define here.[6] We start with defining "seclusive-WHVSV privacy" (Fig.1), that is more extreme and (perhaps) less common, but simpler to define.

Definition 1 – seclusive WHVSH privacy:

Group G has seclusive-WHVSV privacy if and only if

1) There is a set of facts, *I* that includes facts about one or more members of G.
2) All facts in *I* are known by all members of the group and by no one else outside the group $G^C$.[7]

[6] Logically speaking, it is possible to define a vast array of different forms of WHVSV privacy by weakening either the definition of the boundary of the group, e.g. through fuzzy set theory, or of the accessibility of information for outsiders.

[7] Using notation borrowed from set theory, here we use $G^C$ to indicate G's complement, i.e., all the objects that do not belong to set G.

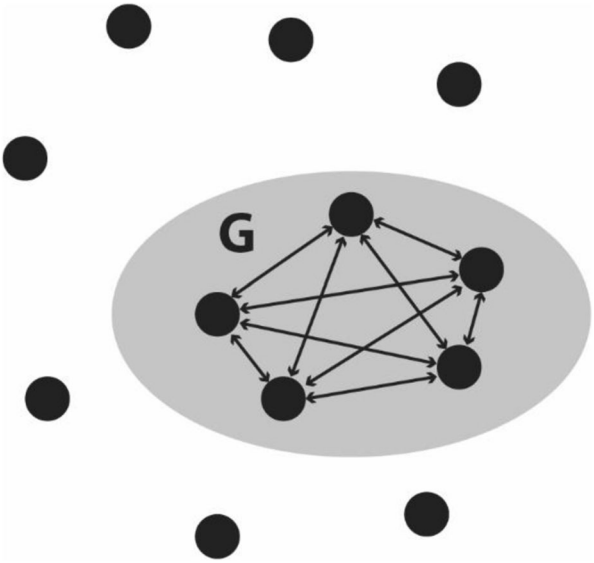


**Fig. 1** Seclusive group privacy. Absolutely private information about the group G is shared only between insiders (circles in the oval) but not with outsiders (circles outside the ovals); an arrow connecting insiders indicates that those two insiders know about each other's private information

Notice that all definitions of group privacy in this paper follow Ruth Gavison (1984), Jeffrey Reiman (1976), and others (e.g., Altman 1976; Moore 2003) in defining privacy as a condition measured in terms of the degree of access others have to the self or information (in this case, information about the members of the group). Analyzing whether a parallel argument can be made based on control definition of privacy, for example, those of Alan Westin (1967), or Fried (1970), is beyond the scope of this paper.

Seclusive privacy is not the most common kind of WHVSV privacy, as we shall see. It is the privacy of a shared secret within a group and the kind of privacy enjoyed, for example, by members of a sect, where all members of a sect know some facts about each other, e.g., the very fact of being member of the sect and other facts that follow from it, which are hidden to everyone else.

We will now show that seclusive-WHVSV privacy satisfies the ontological property discussed by Floridi for it to count as a group feature, in a non-trivial sense which is not being a group of items each of which has that certain feature. (In this sense, having seclusive-WHVSV privacy is not a property of the individuals in the group G, in the same way as "being too heavy to carry" is not a property of individual books.) For example, suppose that Ann, Barbara, Charlotte and Donna, four bachelorettes from Chicago, participate to Ann's transgressive Las Vegas party. After getting drunk, Ann, Barbara, Charlotte, and Donna each reveal to the others in the group one of their most intimate secrets that no one else knows, including their Chicago friends. *I* stands for the set including these facts, the "group-private" facts that are known by all members of the group and no one outside the group; these are, in this specific example, the secrets shared by the four bachelorettes in Las Vegas. Notice that the set of group-private facts is not the set formed by the sum of facts that are individually private for each member

of the group (considered a singleton). For clearly the latter would be the set of purely private facts, known only to the person whose privacy it is and unknown to the other members of the group. The group having group privacy, so defined, clearly does not amount to it being made by members, each of which has individual privacy (understood as the privacy of singleton sets including only the individual whose privacy is in question).

As anticipated, the most common variety of WHVSV privacy is not seclusive privacy. Rather, it is a form that we shall label "antagonistic" privacy. A paradigmatic example of relatively private information is the (American) football huddle (Fig. 2), which is important for football since "the essence of the game is the team strategy communicated in the huddle" (Bloustein 2003, 126). Notice that even when the secrets communicated in the huddle are broadcast to television audiences, this does not destroy the usefulness of group privacy, "so long as the opposition does not learn what is said in time to anticipate the next play" (Bloustein 2003, 126). For another example of antagonistic WHVSV privacy, consider a group of friends out in Vegas for a bachelor party, illustrated in many Hollywood movies. Here, we shall refer to the recent movie The Hangover (Phillips 2009). The character called Alan buys memory-erasing drugs from a drug dealer, the one called Stu marries a stripper, and three of them together, Alan, Stu, and Phil steal Mike Tyson's tiger. After a memory loss, making these events hard to reconstruct, eventually, all four friends find out together the way each of them spent their nights. In this story, it matters for the future well-being of the group that information about Vegas does not reach a specific group of outsiders $G_A$, which is a subset of all outsiders ($G^C$; i.e., $G_A \subset G^C$): wives, fiancées, friends, and acquaintances back home. This is what the expression "what happens in Vegas stays in Vegas" plausibly refers to. Antagonistic privacy is not reduced if the "shared secret" about the group is shared with people who are not part of the group, provided that they do not belong to the "antagonist" group (i.e., $G^C \setminus G_A$). In this case, for example, what happens in Vegas is known by the drug dealer, the stripper, the priest celebrating the Las Vegas wedding, Mike Tyson, and the Las Vegas Police (see Fig. 3). Plausibly, most real-world cases of WHVSV privacy are antagonistic, not seclusive. One can define "antagonist" WHVSV privacy as follows:

Definition 2 – antagonist WHVSV privacy:

Group G has antagonistic WHVSV privacy against a distinct group, $G_A$, if and only if:

1) There is a set of facts, *I* that includes personal facts about one or more members of G.
2) All facts in *I* are known by all members of the group and by no one else in group $G_A$.

As the reader can verify, information that is relatively group-private relative to G against $G_A$ does not coincide with the sum of information about G's members that is relatively private against $G_A$. The reader can easily check that this is the case (to grasp why, notice that absolutely private information can be defined as a special case of relatively private information, where the antagonist group, $G_A$, is the set of all non-members to G, $G^C$).

**Fig. 2** Football huddle. © Marie-Lan Nguyen / Wikimedia Commons

Thus, the two forms of group privacy, both seclusive-WHVSV and antagonistic WHVSV privacy, justify Floridi's ideas that it makes sense to speak about group privacy in a strong sense, such that a group having it, is not the same as a group having individuals each of whom has individual privacy.

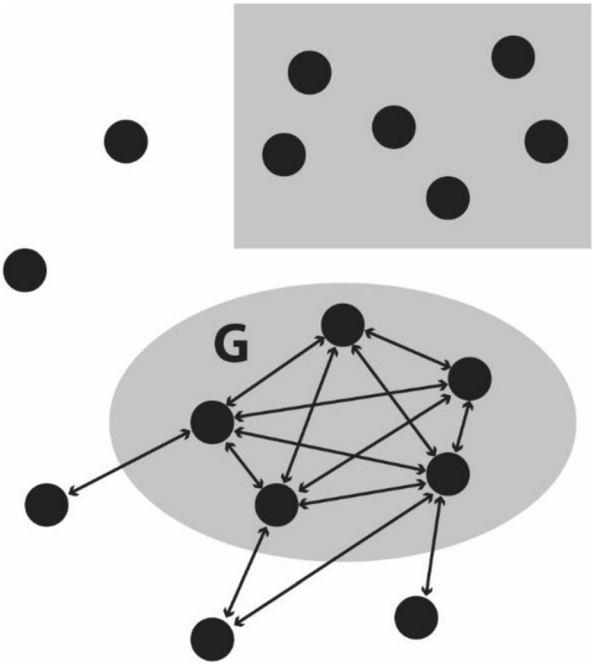


**Fig. 3** Antagonist group privacy: information about the group is shared between insiders (circles in the oval). Information may reach some outsiders (circles outside the box to which arrows point) provided it does not reach the "antagonist" group (circles in the rectangular)

Notice that these two forms of WHVSV do not exhaust the space of logical possibilities of strictly related concepts. The concept of relative-WHVSV privacy may be weakened, further, by considering G, $G^C \backslash G_A$, and $G_A$ as groups with fuzzy boundaries (e.g., some *x* belongs to *G* with a probability *P*) and where the difference between G, $G^C \backslash G_A$, and $G_A$ is in terms of ease with which information flows across such boundaries (again, a matter of different probabilities, rather than a binary condition).

Not only it is perfectly natural to speak of group privacy in this sense, but it is also easy to understand why individuals have an interest in it. Arguably, both forms of WHVSV privacy protect:

> The desire and need of people to come together, to exchange information, share feelings, make plans and act in concert to attain their objectives (Bloustein 2003, 125).

This interest is protected by group privacy because humans are social animals and, in most cases, human happiness

> requires that people reveal themselves to one another – breach their individual privacy – and rely on those with whom they associated to keep within the group what was revealed. Thus, group privacy protects people's *outer space* rather than their inner space, their gregarious nature rather than their desire for complete seclusion (Bloustein 2003, 125, italics added).

Related ideas are used in Floridi's defense of (strong) group privacy. Echoing Bloustein's idea that group privacy protects a group outer space (Bloustein 2003, 125), Floridi claims that:

> entering into a new supra-agent is a delicate and risky operation, care should be exercised before 'melding' oneself with other individuals by sharing personal information or its source, such as common experiences (Floridi 2016, 96).

Notice that Floridi writes this observation in relation to type-a groups, since the supra-agent results from individuals united by the sharing of private information "implicitly (especially by doing things together), or explicitly, through communication" (Floridi 2016, 96). Thus, this is an instance of "a relation of profound trust that binds the people involved intimately" (Floridi 2016, 96). None of this applies to type-b groups.

The defense of "outer boundaries," to which both Floridi and Bloustein refer to, can be regarded as the precondition for the "construction of an individual's own identity" (Floridi 2016, 96), where the identity in question is the identity of a "new multi-agent individual, the group" (Floridi 2016, 96). One can, then, draw a parallel between individual privacy, which is necessary for individuals to develop individuality[8] and

[8] "The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny […] merges with the mass. […] Such a being, although sentient, is fungible; he is not an individual" (Bloustein 2003, 42).

group privacy that "shields the group's identity" (Floridi 2016, 95). It is entirely plausible, as Floridi suggests, that groups with strong bonds, such as "relatives, friends, classmates, fellows, colleagues, comrades, companions, partners, teammates, spouses and so forth" (Floridi 2016, 96), can become "supra-agents" whose persistence (as the same group entities) needs to be protected from informational events which threaten them.

It is possible to see the value of group privacy being affirmed by the laws of liberal states, even when it is not called by that name. For example, "the prohibition of testimony by one spouse regarding confidential communications with the other" (Bloustein 2003, 131) can be regarded as a legal recognition of the essential importance of confidentiality for the intimate bound of love:

> Lovers give themselves up to each other. They lay bare their innermost feelings to each other, they are lewd and foolish with each other, they stand naked before each other. […] But the premise for giving up individual privacy in love is the feeling that what is shared so intimately will not be broadcast to the world at large. Indeed this is the very condition for achieving intimacy (Bloustein 2003, 125).

Yet, not all forms of group privacy are valued as constitutive of (or instrumental to) a single value or interest: for example, the confidentiality in the attorney-client privilege is valued because it is necessary if people "are to enjoy the full benefits of our system of justice" (Bloustein 2003, 133), the group privacy of autonomous or private associations is valued in liberal-democratic societies "because they constitute independent sources of power and initiative which act to forestall undue accumulation of state power" (Bloustein 2003, 129), confidentiality between patients and physicians (Bloustein 2003, 133) is valued for the sake of patient's health, the one between confessor and priest because for the sake of salvation (or, for non-believers, for spiritual well-being), and the one between informants and journalists (Bloustein 2003, 135) is valued, ultimately, to promote truth-seeking and abuse-disclosing behaviors by them, to the advantage of society as a whole. Notice that one may:

- recognize a concept of WHVSV privacy as a form of group privacy the strong sense, such that a group having group privacy is not equivalent to a group being having members all of which have individual privacy
- even recognize that a right to (some forms) group privacy protects important human interests

and yet

- reject the idea of group privacy as a group right

The idea that group privacy is a right of individuals is the conclusion of Bloustein's (2003) analysis of the concept, as some recent contributors to the debate have emphasized (Taylor 2016, 14; Mantelero 2016, 143). Bloustein's conceptualization of group privacy, which is WHVSV privacy, however, is logically compatible with the idea of group rights. This is not only a logically coherent proposition but also a morally

plausible one, as we argue here. Indeed, the plausibility of Floridi's view of group rights to group privacy derives from the plausibility of this view.

Group rights should be kept conceptually distinct from individual rights that people have by virtue of being members of groups, such as, for example, the rights provided to members of races or ethnic groups by affirmative action laws or the rights of members of universities (Jones 2016). In Floridi's world, group rights have to be "rights that belong only to a group as a group, not to a group insofar as it is constituted by individual persons who enjoy those rights" (Floridi 2016, 90). In the literature on group rights, there is widespread agreement that not every collection of individuals can be, if considered as a group, a right holder: some threshold of unity or identity has to be reached (Jones 2016). According to one class of such theories, the relevant condition is the existence of special bonds among group members (Jones 2016, para. 3).[9] Other theories focus on collective agency, for instance, the theory of "conglomerate collectivities" (French 1984), that applies to organizations that have formalized decision-making procedures.

Other theories, for instance Dwight Newman's (2011), require groups surviving changes in individual membership.[10] The question here is if it is plausible to talk about a group right to group privacy, as a privacy right that at least some groups have (these will be type-a groups, according to our definition, which satisfies either Jones' or French's theory).

According to the interest theory of rights (Wenar 2011), the function of rights is to protect the interests of the right holder. But notice that some of these rights can also, and without contradiction, be considered protections of interest that groups themselves have.[11] The interests of sport teams, political parties, and states are examples of interests associated with groups that survive the replacement of their individual members. Suppose that one of Juventus' players has a personal problem that prevents him from training. Juventus has an interest to prevent people outside the organization from acquiring such knowledge, which may confer a competitive advantage to an opponent. The interest protected by the group privacy of the team is plausibly considered a distinct right of Juventus as a team, a right of the collective, which does not derive from the interests in privacy of the individual player.

The other main theory of the function of rights is the will theory, according to which the function of rights is not to protect interests, but "to give its holder control over another's duty" (Wenar 2011, para. 2.2.2). Again, it is not too implausible to claim that at least some groups, e.g., sport teams, political parties, colleagues, charitable associations, have forms of group agency that enable them to exercise control over the duties of others. For example, suppose that the bachelorette group forms a private group on WhatsApp, with one of them as administrators. Any change in the membership of the group, in particular, adding members, would have to be decided by the group administrator as a group representative. Arguably, the individual who acts as a group representative exercises the group authority in ways that alter the duties of added members.

Summing up, we have provided two definitions of WHVSV privacy both of which are coherent with Floridi's claims that there is more to group privacy than the collection of individuals each with their own privacy. Moreover, we have argued that it is not implausible to regard groups, at least in certain cases, as the right holders of a right to

[9] Examples of these are Galenkamp's (1993) or McDonald's (1991) theories.

[10] Some of Floridi's examples of group privacy share this feature.

[11] Some legal scholars and philosophers, for example, Jovanović (2012), May (1989), and McDonald (1991), have claimed groups can have interests.

group privacy. We now turn to another type of group privacy that becomes increasingly important in the realm of big data analytics and typically affects type-b groups.

## 3 Group Privacy, Inferential Privacy, and Big Data

According to Floridi, the question of group privacy is important in the light of privacy threats posed by big data analytics, because big data "is more likely to treat types (of customers, […]), rather than tokens (you, […]), and hence groups rather than individuals (Floridi 2016, 97). By contrast "our current ethical approach is too anthropocentric (only natural person count) and nominalist (only the single individual person counts)" (Floridi 2016, 98, italics added).

Floridi brings attention to "the risks involved in opening *anonymised* personal data to public use in cases in which groups of people may still be easily identified and targeted" (Floridi 2016, 98, italics added). Floridi's concept of group privacy is supposed to apply to sets of persons that are "grouped algorithmically" (Taylor 2016, 15), like "owners of such and such kind of car, shoppers of such and such kinds of goods […]."(Floridi 2016, 97). As Linnet Taylor observes, "the groups created by profiling using large datasets are different from conventional ideas of what constitutes a group in that they are not self-constituted but grouped algorithmically" (Taylor 2016, 14–15). Groups clustered by algorithms, or defined by a feature vector that supports a prediction, are often constituted by individuals who may not have shared any prior interaction (Taylor 2016, 15). They are often type-b groups as we defined them. When predictive models are generated with machine learning, these models can be used to make predictions about a potentially infinite group of people who share a single feature or combination of features. Thus, many predictive models convey knowledge about groups (defined by a feature or set thereof), that are often type-b groups.

The problem predates big data analytics. Virtually, all forms of generalizable knowledge (henceforth, GK) may expose groups to special threats. For example, the discovery that cancer causes smoking exposes all smokers to higher insurance prices. Linnet Taylor has argued that group privacy in the big data domain is a novel phenomenon, because the groups in question are "a new epistemological phenomenon generated by big data analytics" (Taylor 2016, 14). Admittedly, there are differences between knowledge generated through big data analytics in several new applications and traditional methods in epidemiology or clinical medicine. But the ultimate goal of all scientific research is to produce GK, not just knowledge of the research subjects involved in the study. By virtue of GK extracted from some individuals in a group, inferences about other individuals in the group can be made. We thus maintain that the essential ethical problem is how to deal with GK and whether the production of new GK (through big data or other methods) counts as an infringement of "group privacy." We now proceed to provide a definition of group privacy that is pertinent to the issue at stake, where (type-b) groups are identified by any feature (or combination thereof) individuals have in common, which is represented as the result of applying an algorithm, or used in an algorithmic decision.

Definition 3 – inferential group privacy:

The inferential privacy of an entity (individual or group) X, is a measure of the logically valid inferences, about the *sensitive features* of X, that *cannot* be made about X, based on the available data about X.

Sensitive features—in this definition—can be defined as features "which most individuals in a given society at a given time do not want widely known about themselves" (Parent 1983, 269–70) and as the feature that a specific X does not want to be revealed about him/her/itself.

It seems clear that inferential privacy and WHVSV privacy are distinct concepts, even if they are both conditions of restricted access to (the self or) information about the self. Thus, the fact that some groups (e.g., type-a groups) have rights to WHVSV does not entail that other groups (e.g., type-b groups) have rights to inferential privacy. We will now analyze inferential privacy to determine whether a right to inferential privacy is morally plausible and whether the right holders should be considered individuals, or groups, or both.

## 4 Is there a Moral Right to Inferential Privacy?

We will now briefly discuss the objection that there is no absolute right to inferential privacy, irrespective of whether this is conceived as a right of individuals or groups. An absolute right to inferential privacy entails a duty of other people not to draw valid inferences based on the information that an individual reveals publicly, or to them. The idea of an absolute right of this kind is problematic for at least two reasons. First, some philosophers have argued that people lose any right to privacy to information that they make public, whether intentionally or not (Thomson 1975). Suppose you forget a picture in a place where everyone can see it. It seems counterintuitive that you have a right that others do not look at it.[12]

Second, suppose that some scientist *S* knows that person *M* belongs to the group G and she is in the position to discover the generalizable knowledge (GK), which will eventually become public, that all *x* who are *G* have the sensitive feature *F* (F can also be a propensity, with a probability). An absolute right to inferential privacy gives *M* a claim right, that is, entails a duty of S not to generate (GK). This appears problematic because it basically would make most of social science research (or public health research) impossible. It seems unreasonable to confer such power to a member of *G* or to all of its current members. If smokers had such right, they could have prohibited the discovery of the GK that smoking increases cancer risk. It seems unreasonable that an epidemiological study about the relation between smoking and cancer should be authorized by existing smokers individually or collectively. After all, this knowledge has an impact on the well-being of all potential smokers and on future generations. The interests of all potential, present and future, smokers (and non-smokers) may not coincide with the current interests of actual smokers (who may be unable to quit smoking, and whose priority may be to avoid paying higher insurance prices).

An absolute right is also problematic because it entails the duty to avoid drawing spontaneous inferences, for example, deducing that someone you know well has lost her job based on various cues (Rumbold and Wilson 2018, 13). If an observer cannot help drawing an inference from available generalizable knowledge and public information, it is unreasonable to demand that she does not draw it, since "ought" implies "can."

These arguments show that there is no such thing as an absolute right to inferential privacy, but they do not show that there cannot be a more limited right, e.g., a right to

[12] However, it might be a matter of politeness after having spotted the image not to look to closely at the picture. This politeness may reflect a moral duty to respect privacy. Recently, it has been argued (Rumbold and Wilson 2018) that Thomson's argument is invalid because a person cannot waive a right to privacy except by an intentional act.

the maximum degree of inferential privacy which can be achieved without imposing unreasonable costs and limitations on others.[13] One problem about such limited right is that its boundaries will often be unclear. Yet, we will concede here for the sake of the argument that some boundaries can be defined.

## 5 Is the Right to Inferential Privacy a Group Right?

Let us grant, for the sake of the argument, that there is such thing as a right to inferential privacy, understood as the right to the maximum degree of inferential privacy which can be achieved without imposing unreasonable costs and other limitations on others. It may still be asked, whether this is a right that groups or individuals have. If such right exists, it is—we shall argue—more plausibly considered an individual right.

First of all, this is because most algorithmically selected groups are what we have labeled type-b groups—they lack "the stronger taste of a 'we'", in Floridi's (2016, 96) own words. As algorithmically selected individuals may not, and most often do not, experience "the nature of such a bond" (Floridi 2016, 96), as that of families, spouses, and team members. As Linnet Taylor emphasizes, algorithmically selected groups "are not necessarily aware that they belong to [a group]" (Taylor 2016, 15). Awareness to group membership is even less likely to occur in so far as the asset of big data is that we can create feature vectors of many unrelated features in order to have sufficient prediction power—but those groups are even much more artificial than the example "smoker" mentioned here. A group consisting of feature such as drives red car, eats rice, and has long hair may lead to precise predictions, but is plausibly not a good basis for shaping group identities.

As mentioned above, there are two main theories about the function of rights, the interest theory and the will theory. According to the interest theory, a right's function is to protect the interests of the right holder. But in the case of b-groups, these shared interests are mere aggregate interests, which do not reflect a pre-existent bond, possibility of collective action, or group self-awareness. There is no supra-individual agent who can will anything, no idea of a common good. There are at most the shared interest of the individual members forming the group, which can be aggregated.[14]

It is useful to illustrate some differences between algorithmic processes that generate type-a groups and type-b groups. In the early days of Facebook, if one listed some musical group as an interest, it would generate a clickable link. Clicking on it would display all people who had listed the same group as an interest. Arguably, this was an efficient way to

[13] This is also Rumbold and Wilson's conclusion, which accepts that individuals only have a right to a reasonable degree of control over their information, which can be inferred from public information, and that you may make your right to privacy defunct by acting in a way that makes it impossible (or too costly, we shall add) for anyone to discharge the duties associated with such right (Rumbold and Wilson 2018, 17–18). It may also be compatible with the recent idea of a right to reasonable inferences, but we cannot discuss here the details of this legal conception (Wachter and Mittelstadt 2018).

[14] The point can be formulated in terms of Newman's (2004) distinction between aggregate (shared) interests vs. and collective ones, also referred in Mantelero (2016). A collective interest is defined as "a factor that contributes toward the continued collaboration of the members of a community as viable and reasonable" (Newman 2004, 140). By definition, however, b-groups do not have continued community features. For this reason, we object to Alessandro Mantelero's view that "this atomistic and fragmented dimension [of algorithmically linked individual interests] demands a collective representation" (Mantelero 2016, 150) for the general case.

find and create non-previously existing communities defined by shared interests, e.g., the interest in relatively unknown indie groups (Madrigal 2019). The resulting communities could become type-a groups, because the Facebook link generated awareness in these individuals, of the link between them. This group self-awareness matched a viable social identity as "fans of the same musical group," which is meaningful, at least in US culture. We do not object to the idea that this algorithmic process can support a collective identity, as such. We object only to the idea of a (collective) group interest in type-b groups, which by definition do not have such awareness.

Let us now consider the question from the standpoint of the will theory of rights. According to the will theory, the function of a right is to determine who has the power to control other people's duties. Thus, right holders should, at least in principle, be the kind of entity that can exercise such control (Wenar 2011, 2.2.2). A clear objection against group rights to inferential (group) privacy is that an algorithmically sorted group that is a type-b group cannot exercise the required degree of control, because it is formed by individuals who are not even aware of themselves as a group. The moment they organize themselves, they have already changed into a type-a groups.[15]

Wrapping up, even conceding, that there is a right to inferential privacy, assigning this right to type-b groups is typically not morally justifiable. It may be objected that groups, even b-groups, that are created "from outside" (e.g., by algorithmic processes), have an interest not to be treated as groups. An example could be inferences that could be made, through algorithms, concerning sexual orientation, in a society in which homosexuality is kept hidden, experienced with guilt, not acknowledged as a possible human relation, stigmatized, and criminalized. In this hypothetical society, let us suppose, homosexual inclinations do not constitute a viable form of human sociality. Let us also imagine a society that is not aware of other ways of experiencing homosexuality, as its members do not have *inter alia* access to information about cultures where it is experienced differently.

It may well be conceded that individuals in this group may have an interest not to be treated as a group, e.g., a group that is discriminated. But in this specific society, the group interest in question is a mere shared interest, the aggregation of similar individual interests. It is not a collective interest in the sense that presupposes the possibility of group interaction, at least in planning or in the imagination (D. G. Newman 2004, 140).[16] From the point of view of the will theory—which identifies the right holder as the agent exercising the right—a group right has no function here, as, by hypothesis, there is no organization or group representative. If "a procedural right to a judicial remedy against the data controllers"(Pagallo 2016, 163) should exist, it seems logical that it should be exercised by individuals, or by third parties in the name of individuals (who happen to form a group, or better a set).[17] For a different representation to be justified, the group has to, at a minimum,

[15] Moreover, even when the organization is feasible, these rights will typically be limited, not absolute, as the example of the smokers above shows.

[16] See note 14 on the difference between the two.

[17] Our point is not merely that group rights may conflict with individual rights. Even if "the aim of this protection is […] to complement the [legal safeguard of individual privacy] with [a privacy group regime]"(Pagallo 2013, 165), our position is that in the case of b-groups there is no (non-merely aggregative) group interest to protect. There is also no group right to be exercised by groups, or on their behalf. We also object to the proposal of collective representation exercised by data protection authorities (Mantelero 2016, 151). The adjective "collective," here, points to individual rights that people have by virtue of being members of groups, such as, for example, the rights provided to members of races or ethnic groups by affirmative action laws. We do not use the expression "group rights" for these rights.

acquire awareness of itself *qua* group. This may happen as a consequence of overt profiling and discrimination, but it does not have to. If the group identity emerges, the group becomes a type-a group, according to our definition. We have no issue against the claim, that an algorithmically sorted group should have the right "to develop their identity and promote their interests as a group" (Van der Sloot 2016, 222), if the members want it. But if they want this, they represent themselves already as a group, and, thus, qualify already as a type-a group.

## 6 Conclusions

In this paper, we have distinguished two concepts of group privacy, namely "what happens in Vegas stays in Vegas" (WHVSV) privacy and inferential privacy. We have argued a right to group privacy is most plausible in relation to the WHVSV privacy of type-a groups (groups which have a history of interactions or non-trivially shared goals). By contrast, what is threatened by big data analytics is especially the inferential privacy of individuals that are characterized by features common to open-ended groups. An absolute right to inferential privacy, we have argued, is implausible to begin with. If a limited right is plausible, it is not plausible as a group right (in the strong sense) of algorithmically defined type-b groups.

Both concepts of group privacy (WHVSV privacy and inferential privacy) have important implications for information and communication technology. Rights to absolute or antagonistic WHVSV privacy have been implemented already in many communication platforms, with both beneficial and harmful consequences for society. Take, for example, private groups on Facebook and group chats on WhatsApp, the technology behind these allows groups to define, by themselves, boundaries between insiders and outsiders, which is crucial for WHVSV privacy. Such groups can be beneficial because they facilitate the expression of minoritarian views and improve the welfare of minority members that may otherwise feel overwhelmed and intimidated by majorities. But they can also be harmful to society when they become echo chambers for favor extreme views and polarization (Sunstein 2017).

The concept of a right to inferential group privacy is important in relation to big data analytics, for reasons eminently spelled out by Floridi in the paper considered here and the surrounding literature. But it also seems that the allegedly special threat against the inferential privacy of groups (compatible with the anonymization of individuals in those groups) can be reduced to a more familiar problem about harmful uses of generalizable knowledge. Such knowledge potentially affects many more people besides the limited sample which enabled the generation of such knowledge. One possible conclusion is that not all forms of privacy can be protected by giving individuals, or groups, rights to control information. On the contrary, inferential privacy requires a vision of the societal impact of knowledge generation, which crucially, researchers and other users of big data analytics also (perhaps, mainly) have the responsibility to develop.

**Acknowledgments** The authors wish to thank participants to the senior academic session at CPDP 2019 and one anonymous referee of this journal for useful feedback.

**Funding Information** The project has been supported by a Grant of the Swiss National Research 75, grant-number: 407540_167218 and has received funding from the European Union's Horizon 2020 research and innovation programme under agreement NO 700540 and by the Swiss state Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1.



## References

Altman, I. (1976). Privacy: a conceptual analysis. *Environment and Behavior, 8*(1), 7–29.

Bloustein, E. J. (2003). *Individual and group privacy* (2nd ed.). New Brunswick: Routledge.

Floridi, L. (2014). Open data, data protection, and group privacy. *Philosophy & Technology, 27*(1), 1.

Floridi, L. (2016). group privacy: a defence and an interpretation. In L. Taylor, L. Floridi, & B. Van der Sloot (Eds.), *Group privacy: new challenges of data technologies* (pp. 83–100). Cham: Springer.

French, P. A. (1984). *Collective and corporate responsibility*. New York: Columbia University Press.

Fried, C. (1970). *An anatomy of values: problems of personal and social choice*. Harvard University Press.

Galenkamp, M. (1993). *Individualism versus collectivism: the concept of collective rights*. Rotterdam: Erasmus Universiteit, Faculteit der Wijsbegeerte.

Gavison, R. (1984). Privacy and the limits of the law. In F. D. Shoeman (Ed.), *Philosophical dimensions of privacy: an anthology*. Cambridge: Cambridge University Press.

Hildebrandt, M. (2013). Balance or trade-off? Online security technologies and fundamental rights. *Philosophy & Technology, 26*(4), 357–379. https://doi.org/10.1007/s13347-013-0104-0.

Jones, P. (2016). Group rights. In E. N. Zalta (Ed*.), The Stanford encyclopedia of philosophy*. Summer 2016. Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/sum2016/entries/rights-group/.

Jovanović, M. A. (2012). *Collective rights: a legal theory*. Cambridge: Cambridge University Press.

Madrigal, A. C. (2014). *How Netflix reverse engineered Hollywood*. The Atlantic, January 2, 2014. http://www.theatlantic.com/technology/archive/2014/01/how-netflix-reverse-engineered-hollywood/282679/.

Madrigal, A. C. (2019*). Before it conquered the world, Facebook conquered Harvard*. The Atlantic. February 4, 2019. https://www.theatlantic.com/technology/archive/2019/02/and-then-there-was-thefacebookcom/582004/.

Mantelero, A. (2016). From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era. In L. Taylor, L. Floridi, & B. Van der Sloot (Eds.), *Group privacy: new challenges of data technologies* (pp. 139–158). Cham: Springer.

May, L. (1989). *The morality of groups: collective responsibility, group-based harm, and corporate rights*. Notre Dame: University of Notre Dame Press.

McDonald, M. (1991). Should communities have rights? Reflections on Liberal individualism. *Canadian Journal of Law & Jurisprudence, 4*(2), 217–237.

Moore, A. D. (2003). Privacy: its meaning and value. *American Philosophical Quarterly, 40*(3), 215–227.

Newman, D. G. (2004). Collective interests and collective rights. *American Journal of Jurisprudence, 49*, 127.

Newman, D. (2011). *Community and collective rights: a theoretical framework for rights held by groups*. Oxford: Bloomsbury Publishing.

Pagallo, U. (2013). Online security and the protection of civil rights: a legal overview. *Philosophy & Technology, 26*(4), 381–395. https://doi.org/10.1007/s13347-013-0119-6.

Pagallo, U. (2016). The group, the private, and the individual: a new level of data protection? In L. Taylor, L. Floridi, & B. Van der Sloot (Eds.), *Group privacy: new challenges of data technologies* (pp. 159–173). Cham: Springer.

Parent, W. A. (1983). Privacy, morality, and the law. *Philosophy & Public Affairs, 12*(4), 269–288.

Phillips, T. (2009). *The Hangover*. Comedy. http://www.imdb.com/title/tt1119646/. Accessed June 25 2018.

Reiman, J. (1976). Privacy, intimacy and personhood. *Philosophy and Public Affairs, 6*(1), 26–44.

Rumbold, B., & Wilson, J. (2018). Privacy rights and public information. *Journal of Political Philosophy* online first (0). https://doi.org/10.1111/jopp.12158.

Sunstein, C. R. (2017). *#Republic: divided democracy in the age of social media*. Princeton: Princeton University Press.

Taylor, L. (2016). Safety in numbers? Group privacy and big data analytics in the developing world. In L. Taylor, L. Floridi, & B. Van der Sloot (Eds.), *Group privacy: new challenges of data technologies* (pp. 13–33). Cham: Springer.

Thomson, J. J. (1975). The right to privacy. *Philosophy & Public Affairs, 4*(4), 295–314.

Van der Sloot, B. (2016). Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under article 8 ECHR. In L. Taylor, L. Floridi, & B. Van der Sloot (Eds.), *Group privacy: new challenges of data technologies* (pp. 159–173). Cham: Springer.

Wachter, S., B. D. Mittelstadt. (2018). A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220. https://doi.org/10.2307/1321160.

Wenar, L. (2011). Rights. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy*. Fall 2011. http://plato.stanford.edu/archives/fall2011/entries/rights/.

Westin, A. F. (1967). *Privacy and freedom* (1st ed.). New York: Atheneum.